

CLAIMS

WHAT IS CLAIMED IS:

1. A method comprising:
 - receiving, via at least one processor and at a first entity, a first algorithm subset from
5 an algorithm provider, the first algorithm subset representing a first portion of an algorithm that is less than the entire algorithm;
 - receiving, via at least one processor and at a second entity, a second algorithm subset from the algorithm provider, the second algorithm subset representing a second portion of the algorithm that is less than the entire algorithm, wherein the second portion of the algorithm
10 differs from the first portion of the algorithm;
 - generating, via the first entity, two shares of a first mathematical set based on a first parameter associated with the first algorithm subset;
 - transmitting at least a portion of the two shares of the first mathematical set from the first entity to the second entity;
 - 15 generating, via the second entity, two shares of a second mathematical set based on a second parameter associated with the second algorithm subset;
 - transmitting at least a portion of the two shares of the second mathematical set from the second entity to the first entity;
 - receiving, at the first entity, a first split data subset of a full data set;
 - 20 receiving, at the second entity, a second split data subset of the full data set;
 - running the first algorithm subset on the first split data subset based on the two shares of the first mathematical set to yield a first output subset;
 - running the second algorithm subset on the second split data subset based on the two shares of the second mathematical set to yield a second output subset; and
 - 25 combining the first output subset and the second output subset.

2. The method of claim 1, wherein the first algorithm subset from the algorithm that has been divided into a third algorithm subset and a fourth algorithm subset.
3. The method of claim 1, wherein the first parameter comprises a first characteristic of the first algorithm subset and wherein the second parameter comprises a second characteristic of the second algorithm subset.
4. The method of claim 1, wherein the first parameter relates to a nature of the first algorithm subset and wherein the second parameter both relate to a nature of the second algorithm subset.
5. The method of claim 1, wherein the first split data subset is generated randomly as part of the full data set.
6. The method of claim 1, wherein the second split data subset is generated randomly as part of the full data set.
7. The method of claim 1, wherein the first entity and the second entity comprise one of two physically separate computing device or two separate virtual computing devices.
8. The method of claim 1, wherein each of the first mathematical set and the second mathematical set comprise a beaver set.
9. The method of claim 1, wherein each of the first mathematical set and the second mathematical set comprise an NxM matrix.
10. The method of claim 1, wherein the running of the first algorithm subset on the first split data subset based on the two shares of the first mathematical set to yield the first output subset and the running of the second algorithm subset on the second split data subset based on the two shares of the second mathematical set to yield the second output subset occur using a memoization technique.
11. A system comprising:
- at least one processor; and
- a computer-readable storage medium storing instructions which, when executed by the at least one processor, cause the at least one processor to perform operations comprising:

receiving, at a first entity, a first algorithm subset from an algorithm provider, the first algorithm subset representing a first portion of an algorithm that is less than the entire algorithm;

5 receiving, at a second entity, a second algorithm subset from the algorithm provider, the second algorithm subset representing a second portion of the algorithm that is less than the entire algorithm, wherein the second portion of the algorithm differs from the first portion of the algorithm;

generating, via the first entity, two shares of a first mathematical set based on a first parameter associated with the first algorithm subset;

10 transmitting at least a portion of the two shares of the first mathematical set from the first entity to the second entity;

generating, via the second entity, two shares of a second mathematical set based on a second parameter associated with the second algorithm subset;

15 transmitting at least a portion of the two shares of the second mathematical set from the second entity to the first entity;

receiving, at the first entity, a first split data subset of a full data set;

receiving, at the second entity, a second split data subset of the full data set;

running the first algorithm subset on the first split data subset based on the two shares of the first mathematical set to yield a first output subset;

20 running the second algorithm subset on the second split data subset based on the two shares of the second mathematical set to yield a second output subset; and

combining the first output subset and the second output subset.

12. The system of claim 11, wherein the first algorithm subset from the algorithm that has been divided into a third algorithm subset and a fourth algorithm subset.

25 13. The system of claim 11, wherein the first parameter comprises a first characteristic of the first algorithm subset and wherein the second parameter comprises a second characteristic of the second algorithm subset.

14. The system of claim 11, wherein the first parameter relates to a nature of the first algorithm subset and wherein the second parameter both relate to a nature of the second algorithm subset.

15. The system of claim 11, wherein the first split data subset is generated randomly as
5 part of the full data set.

16. The system of claim 11, wherein the second split data subset is generated randomly as part of the full data set.

17. The system of claim 11, wherein the first entity and the second entity comprise one of two physically separate computing device or two separate virtual computing devices.

10 18. The system of claim 11, wherein each of the first mathematical set and the second mathematical set comprise a beaver set.

19. The system of claim 11, wherein each of the first mathematical set and the second mathematical set comprise an NxM matrix.

20. The system of claim 11, wherein the running of the first algorithm subset on the first
15 split data subset based on the two shares of the first mathematical set to yield a first output subset and the running of the second algorithm subset on the second split data subset based on the two shares of the second mathematical set to yield a second output subset occur using a memoization technique.

20

25